IN THE CLAIMS

Please amend the claims as follows.

1. (Currently Amended) A method to remotely validate an email message, comprising:

receiving, at a recipient, the email message in a first encrypted format ~~directly~~ from a sender of the email message;

decrypting, at the recipient, contents of the email message from the first encrypted format;

transferring, from the recipient, the decrypted email message contents to a remote server; and

receiving, at the recipient, from the remote server a status flag, wherein a value associated with the status flag indicates whether the contents are free from a virus or are free from objectionable material as validated by the remote server.

2. (Original) The method of claim 1, further comprising encrypting the email message in a second encrypted format before transferring the email message to the remote server.

3. (Original) The method of claim 1, further comprising accessing the email message for use, if the value of the status flag indicates the remote server validated the email message.

4. (Original) The method of claim 1, wherein in transferring the email message, the first encrypted format is a Secure Multi-Purpose Internet Mail Extension (S/MIME) format.

5. (Original) The method of claim 1, wherein in receiving the status flag, if the value of the status flag indicates the remote server validated the email message, then subsequent accesses made to the email message do not result in the email message being transferred to the remote server for validation.

6. (Original) The method of claim 1, wherein in transferring the email message, the email message is streamed to the remote server.

7. (Currently Amended) A method to validate a data message, comprising:

receiving the data message from a client, wherein the data message was previously ~~directly~~ received at the client and sent from a sender of the data message to the client, wherein the client decrypts the data message before the data message is processed by the client, and wherein the client is external and remote to the method and communicates with the method over a network by sending the data message for scanning;

scanning the data message for viruses; and

sending a validation flag to the client, wherein the validation flag includes a value indicating whether the data message includes zero or more of the viruses.

8. (Original) The method of claim 7, further comprising decrypting the data message before scanning the data message.

9. (Original) The method of claim 8, wherein in decrypting the data message, the data message is decrypted using a public key of the client.

10. (Original) The method of claim 7, wherein in receiving the data message, the data message is an email message and the client is an email client.

11. (Original) The method of claim 7, wherein in receiving the data message, the data message is received from an operating system residing on the client.

12. (Original) The method of claim 7, wherein in scanning the data message, a scanning set of executable instructions is selectively executed to scan the data message for zero or more of the viruses.

13. (Original) The method of claim 7, wherein in receiving the data message, the data message is received as a data stream from the client and scanned as the data stream is received.

14. (Currently Amended) An email system to validate an email message, comprising:

a local email set of executable instructions residing on a client;

a remote validation set of executable instructions residing on a server; and

wherein the email message is received by the local email set of executable instructions ~~and received directly~~ from a sender, who intends the email message for the client, and local email set of executable instructions decrypts the email message~~, decrypted,~~ and then ~~streamed~~ streams the email message to the remote validation set of executable instructions located on the server in an unencrypted format or in a different encrypted format from what was received on the client from the sender and wherein the email message is scanned and a validation flag associated with a result of the scan is sent to the local email set of executable instructions back on the client.

15. (Original) The email system of claim 14, wherein the local email set of executable instructions accesses the email message if the result indicates the scan validated the email message.

16. (Currently Amended) The email system of claim 15, wherein the scan validates the email message [[if]] is the email messages is free of viruses.

17. (Original) The email system of claim 14, wherein the local email set of executable instructions removes the data message if the result indicates the scan did not validate the email message.

18. (Original) The email system of claim 14, wherein communications between the local email set of executable instructions and the remote validation set of executable instructions are secure.

19. (Original) The email system of claim 18, wherein public and private key pairs associated with the client and the server are used to encrypt and authenticate the communications.

20. (Original) The email system of claim 14, wherein the email message includes an attachment message and wherein the email message is in a Secure Multi-Purpose Internet Mail Extension (S/MIME) format when received by the local email set of executable instructions.

21. (Currently Amended) An email message residing on a computer readable medium operable to be remotely validated, comprising:

a first encrypted format associated with content data of the email message, wherein an email client, which is an intended recipient of the email message, decrypts the first encrypted format to render the content data, and wherein the first encrypted format is received on the email client ~~directly~~ from a sender of the content data, the sender directs the email message to the recipient; and

a second encrypted format associated with the content data, wherein the email client generates the second encrypted format, and wherein the email client transfers the second encrypted format of the email message to a remote server, which is external to the email client and to an environment of the email client, and wherein ~~where~~ the content data is rendered by and at the remote server by decrypting the second encrypted format, and wherein the remote server scans the content data for viruses.

22. (Original) The email message of claim 21, wherein a validation flag indicating whether zero or more of the viruses are detected in the content data is generated by the remote server and sent to the email client.

23. (Original) The email message of claim 21, wherein the first encrypted format is a Secure Multi-Purpose Internet Mail Extension (S/MIME) format.

24. (Original) The email message of claim 21, wherein the second encrypted format is generated by using a private key for the email client and a public key for the remote server.

25. (Original) The email message of claim 21, wherein the email client accesses the content data for use when the remote server detects no viruses.

26. (Original) The email message file of claim 21, wherein the content data includes text data and attachment data.